Tencent 腾讯 | 腾讯云

腾讯工业互联网平台安全解决方案

产业安全运营部　腾讯安全高级架构师　张乐

1 工业互联网面临的安全风险分析

- **建设背景：**国家高度重视工业互联网、智能制造，地方政府及企业应抓住新基建的重要机遇，实现产业发展升级
- **主要安全风险：**新技术应用、IOT网络融合等，导致边界进一步模糊，安全风险增加

工业互联网定义

- 工业互联网作为全新工业生态、 关键基础设施和新型应用模式。
- 通过**人、机、物**的全面互联，实现**全要素、全产业链、全价值链的全面连接，正在全球范围内不断颠覆传**统制造模式、生产组织方式和产业形态
- 推动传统产业加快转型升级、新兴产业加速发展壮大。

——摘自工业互联网产业联盟《工业互联网体系架构2.0》

工业网互联网与新基建

时间	会议名称	相关内容
2018.12.19	中央经济工作会 议	加快5G、工业互联网等新型基础设施建设，拓展创新技 术的应用场景建设;实施北京智源行动计划，推动人工智 能带动各领域各产业升级和变革。
2019.03.03	“两会”	强化逆周期调节，除了传统基建外,以5G、人工智能和工 业互联网、物联网为代表的新型基建将承担更为重要的角 色。
2019.07.30	中共中央政治局 会议	要稳定制造业投资、实施补短板工程，加快推进信息网络 等新型基础设施的建设。
2020.01.03	国务院常务会议	大力发展先进制造业.出台信息网络等新型基础设施建设投资支持改策，推进智能绿色制造。
2020.02.14	中央全面深化改 革委员会会议	基础设施是经济社会发展的重要支撑,要以整体优化、协同融合为导向,统筹存量和增量传统和新型基础设施发展。打造集约高效经济适用、绿色智能安全可靠的现代化基础 设施体系。
2020.02.21	中共中央政治局 会议	加大试剂、药品、疫苗研发支持力度，推动生物医药、医 疗设备、5G网络、工业互联网等加快发展。
2020.02.23	中央统筹推进新 冠肺炎防控和经 济社会发展工作 部署会议	智能制造、无人配送、在线消费、医疗健康等新兴产业展 现出强大成长潜力.要以此为契机,改造提升传统产业。培 育壮大新兴产业。
2020.03.04	中央政治局常务 委员会会议	要加大公共卫生服务、应急物资保障领域投入，加快5G网络、数据中心等新型基础设施建设速度。

工业互联网平台架构

工业互联网云平台层

设计 | 研发 | 生产 | 销售 | 售后 | 物流 | 管理 | 供应链 | …

平台应用

协同制造 | 学习培训 | 工业电商 | 工业社区 | 智能客服 | 企业门户 | 企业微信 | 驾驶舱 | 供应链金融

应用市场

ERP SRM MES | PLM CAX | IOT 远程运维 | TMS RMS | OA HR CRM | …

运营支撑

平台门户 | 平台租户管理 | 运营商管理 | 客户管理 | 服务商管理 | 商品管理 | 计费管理 | 统一账户 单点登录

PaaS

微服务 | 大数据 | 人工智能 | 云镜 | 数据治理

数据库 | 中间件 | 开发工具 | 蓝鲸 | …

IaaS

计算 | 存储 | 网络 | …

TStack | TCE | ECC

边缘层

边缘层/设备层

核心层运算 (EdgeComputing)

工业等级高阶工作站 | 工业等级储存装置 | 工业等级网络安全设备

工业网关 (Gateway)

工业等级闸道器 | 工业控制IPC

机台控制/监控 (Industrial Control)

传感器/芯片 | 设备监控 CCD/机器视觉 人机界面 运动控制盒 工业手持装置

工厂设备 (Equipment)

设备装置

核心层AI决策

协议解析

OPC UA | TSN

TSN (Time-Sensitive Networking)

KEPServerEX | CODESYS | EtherCAT | Modbus

工业通讯协议

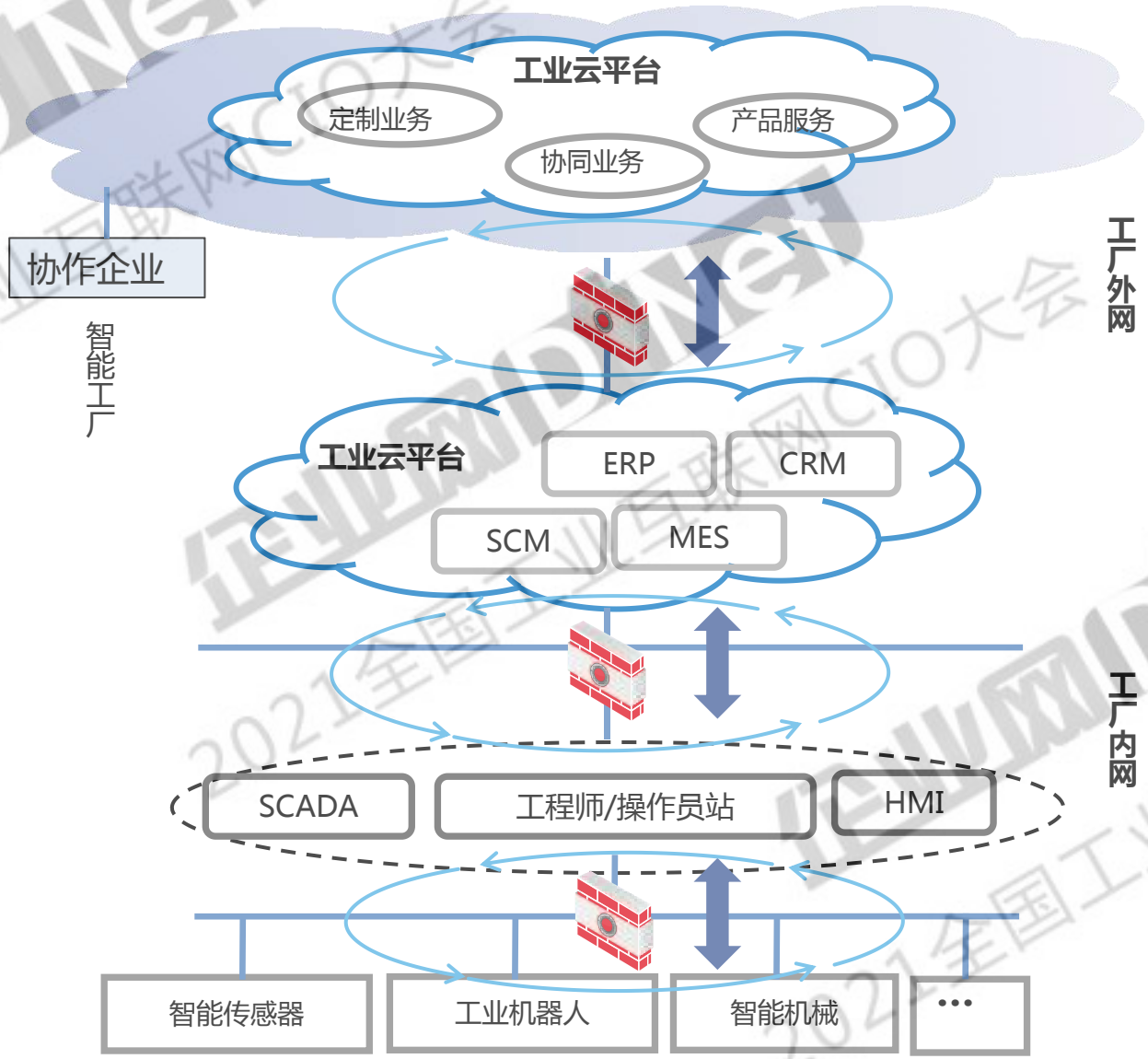
开放互联形势下的工业互联网络安全挑战

控制环境开放化使外部互联网威胁渗透到工厂控制环境

控制安全

网络IP化、无线化以及组网灵活化给工厂网络带来更大的安全风险

网络安全



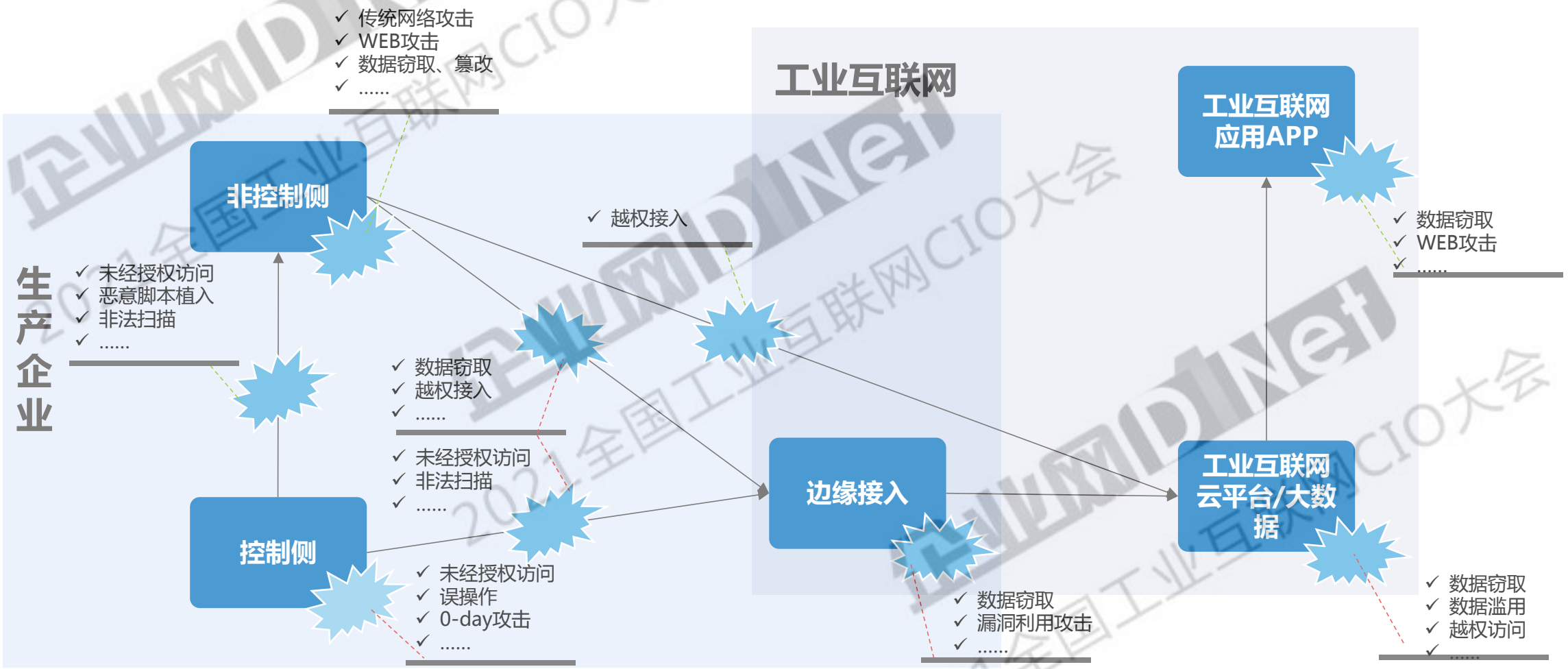
数据的开放、流动和共享使数据和隐私保护面临前所未有的挑战

数据安全

设备智能化使生产装备和产品暴露在网络攻击之下

设备安全

工业互联网业务流程风险分析



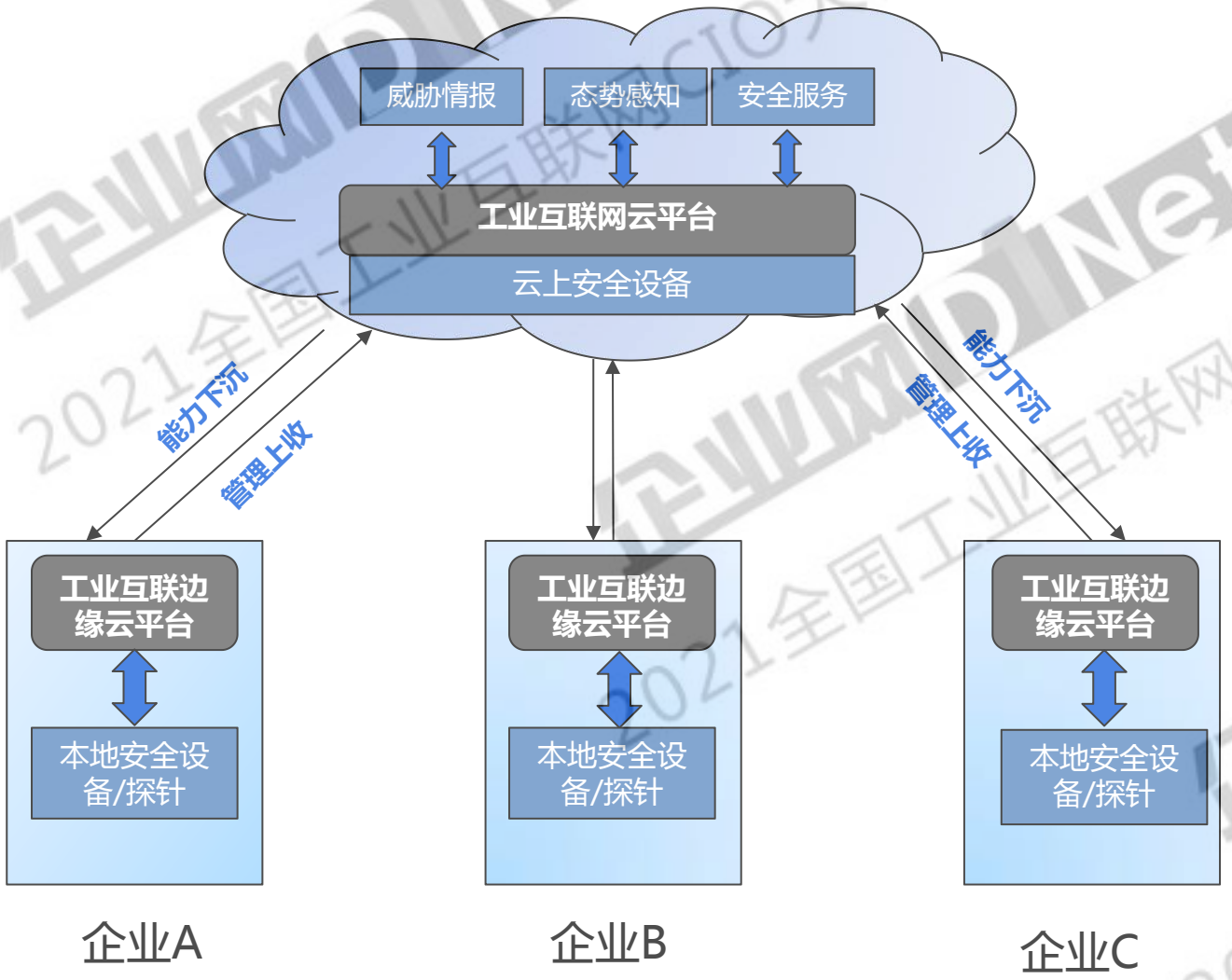
2 工业互联网安全架构

- **传统安全方案：**针对传统安全建设模式存在的问题进行分析
- **解决思路：**提出工业互联网安全建设新思路
- **工业互联网安全架构：**形成IOT一体化的工业互联网安全架构

传统方案落地存在的主要挑战

- 重产品，轻服务
- 重建设，轻运营
- 重防御，轻检测
- 设备堆叠为主，体系化能力不足
- IT安全和OT安全割裂，缺乏统一视图
- 安全人才缺乏，运维能力不足
- 安全价值难以量化

解决思路：“平台+设备+服务”模式



- 构建创新的“**平台+产品+服务**”模式。通过**安全大数据平台**汇集大数据能力；通过云端和本地**安全设备**，形成涵盖从平台侧向企业侧的完整安全能力；通过创新**安全服务**，进一步弥补人才短板，并实现闭环。最终实现的以下效果：
  - **管理上收:**实时汇集企业侧安全设备（网关、代理、agent等）日志数据至云端，基于人工智能、大数据分析技术，实现IOT资产、漏洞及风险的可视化，增加威胁发现能力。
  - **能力下沉：**部分安全设备本地部署，形成涵盖**云、网、应用、数据、终端**的纵深防护能力；整合各方生态，进一步加强安全服务能力下沉，可为企业提供安全运维、风险评估、应急响应等标准化安全服务。

工业互联网安全整体架构

3 腾讯工业互联网安全解方案

- **平台和应用安全：**针对边缘层、IaaS、PaaS、SaaS分层防护
- **网络通信安全：**提升企业内外网的安全防护能力
- **设备和控制安全：**加强工业生产、主机、控制网络协议等安全保障
- **工业数据安全：**加强数据收集、存储、处理、转移、删除等安全保护要求
- **IOT安全运营中心：**基于信息技术（IT）和操作技术（OT）统一安全管理平台，而不干扰任何操作业务过程。
- **安全服务：**提供安全咨询、风险评估、MSS安全托管等服务

平台和应用安全：整体安全框架

安全基础设施

工业SaaS安全
- Web入侵防护
- web防篡改
- Web应用加固
- 漏洞检测
- 数据加密
- 身份认证

工业PaaS安全
- 数据安全：数据加密、数据脱敏、数据权限控制、数据审计
- API安全：API白名单、API调用认证、API漏洞检测、API权限认证
- 容器安全：镜像安全、资源隔离、访问控制、容器防逃逸、安全加固

IaaS安全
- 存储安全：数据分级、数据分类、数据加密、数据防篡改、剩余信息保护
- 云网络安全：虚拟网络访问控制、VPC隔离、网络威胁检测、租户隔离
- 主机安全：访问控制、入侵防护、恶意代码防护、资源控制
- 虚拟化安全：虚拟机防逃逸、虚拟资源隔离、镜像防篡改
- 网络安全：边界访问控制、安全域划分、单向隔离、数据加密、抗DDOS、防恶意代码、设备冗余、入侵监测/防护

边缘计算层接入安全
- 工控设备接入：边界安全、通信加密、设备认证、数据采集、协议分析、日志采集
- 物联网设备接入

物理安全
- 固件安全
- 端口访问控制
- 设备访问控制

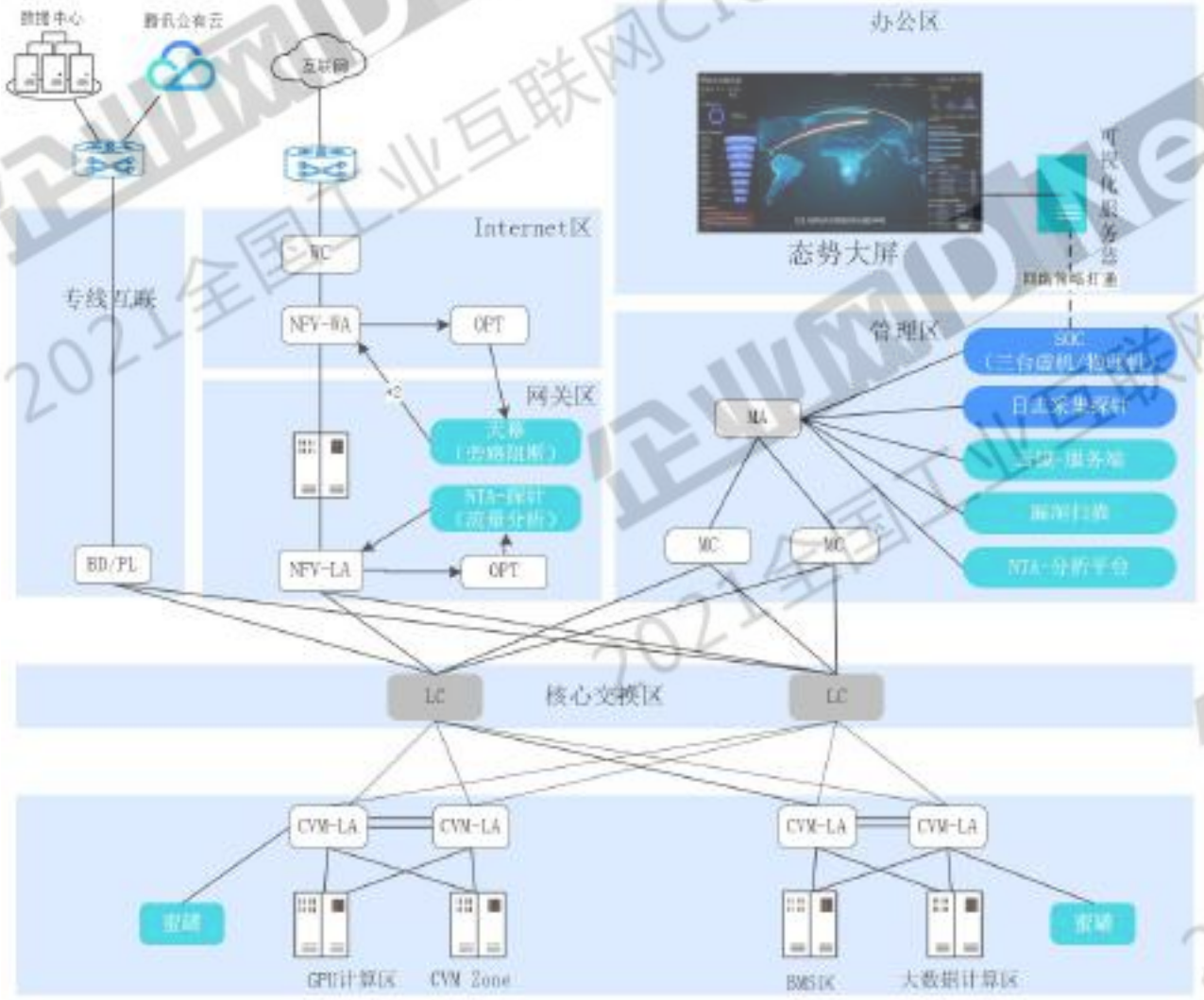
安全运营体系

- 资产管理：IT资产管理、漏洞管理、知识管理
- 基线配置：安全基线管理、安全监测、安全策略管理、通报管理、安全事件管理、预案管理
- 策略控制：风险汇聚、联动通报、分析决策、编排调度、信任评估、策略指令下发
- 态势感知：安全态势、安全风险评估、安全风险预警

- 风险评估：资产安全评估、流量安全评估、合规性评估、评估计划管理
- 零信任服务：环境感知、权限管理、认证服务、业务审计
- 应急响应：事件分析、事件诊断、合规性分析、攻击定位、事件处置、证据固定

- 安全信息感知
- 安全资源管控
- 安全基础资源

平台和应用安全：云平台安全总体部署



1、云平台互联网接入区出口部署**DDoS、防火墙（FW+IPS+AV+负载均衡）**产品。

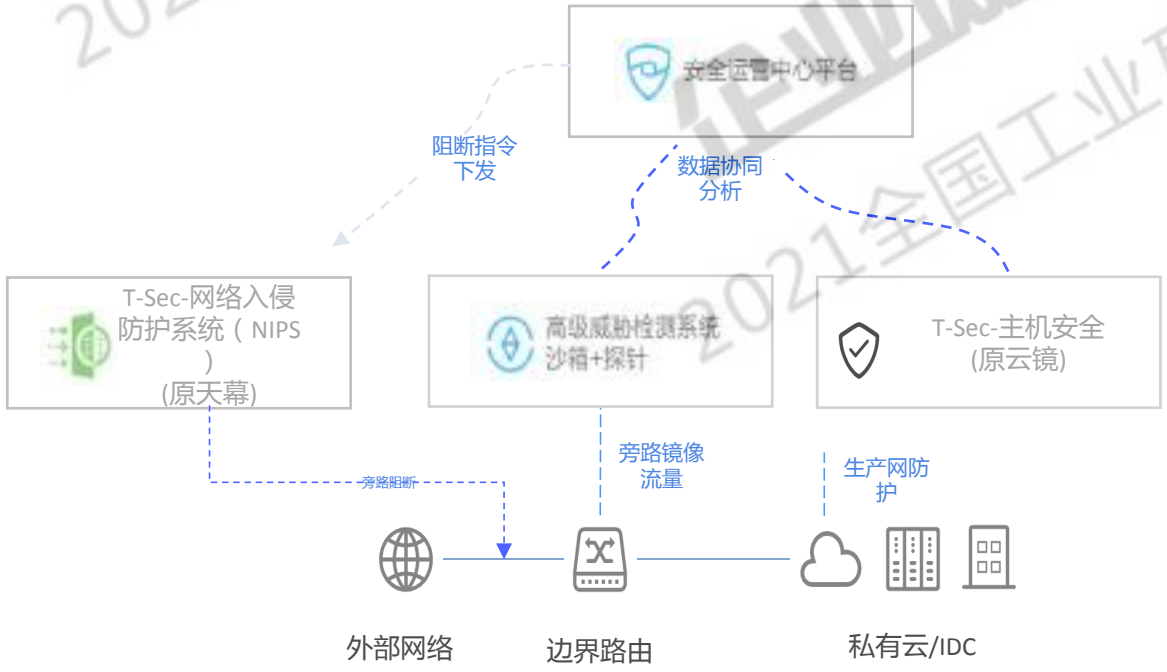
2、在云平台出口核心交换机旁路部署高级威胁感知与处置方案（御界、天幕），实现网络层的**ID/PS、APT感知、AV**等检测与防护能力。

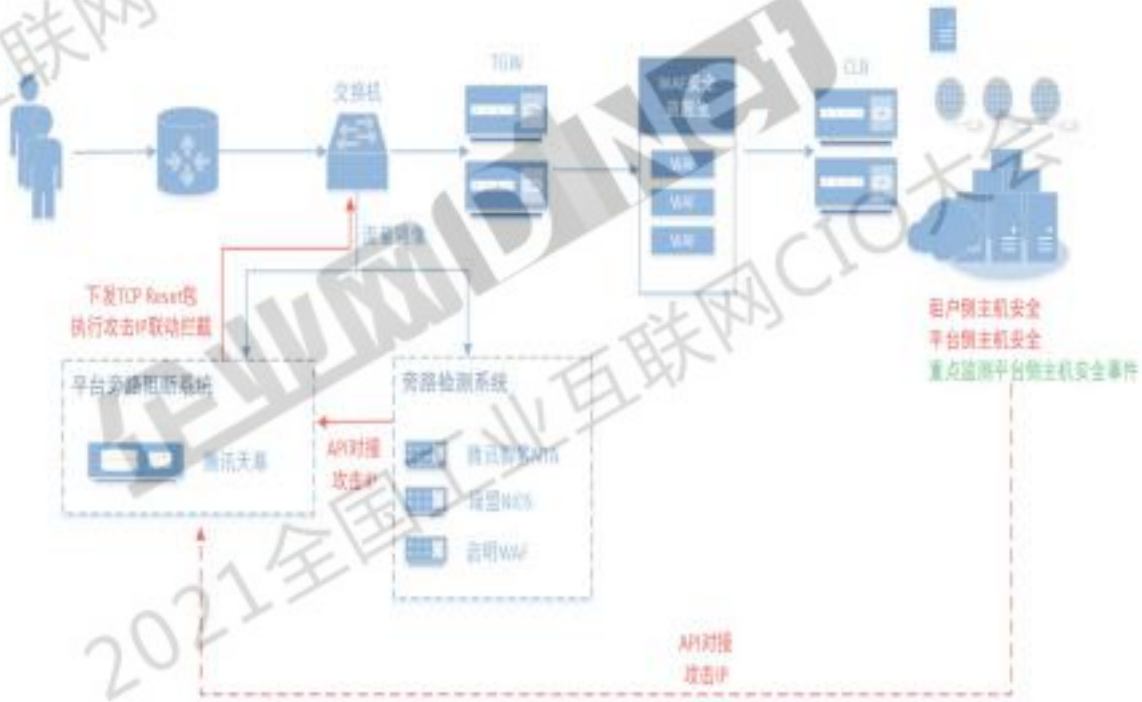
3、在云平台资源层主机部署天眼云镜**CWP产品**，保护资源层主机安全。

4、云平台安全管理区部署**腾讯御见、堡垒机、主机和Web漏扫、数据库审计、日志审计**等产品。

平台和应用安全：云平台安全联动防御

- 针对强攻防对抗场景，要求检测全、阻断快，确保攻防对抗下能看得清、防得住，构建新一代的智能化联动防御体系。
- 通过流量镜像旁路分析云平台恶意流量分析和恶意文件，及时发现异常行为。通过流量分析发现僵尸、木马、蠕虫等非法外联，通过安全沙箱分析未知威胁行为和文件。防止0day和新的攻击行为。
- 通过旁路方式，提供双向流量逐包检测和IP封禁能力，解决数据中心的协同防御和安全治理问题
- 安全检测：NTA、云镜、御点；安全阻断：天幕；智能分析与安全可视：SOC





平台和应用安全：工业应用APP安全

开发运维人员　外部用户　内部用户

身份与访问控制层
- 双因素认证
- 访问控制
- 账号管理
- 操作审计
- 应用管理
- 特权账户
  - 运维审计

应用层
- Web安全
- 小程序安全
- API安全
- 安全配置监测
- 微服务
- 传统业务系统
- API接口

数据层
- 动态脱敏
- 数据加密
- 数据库审计
- TDSQL
- RDB

工作负载层
- 安全基线
- 漏洞修复
- 弱口令
- 云主机
- 容器服务
- 函数计算

用户活动日志　应用访问日志　数据库访问日志　主机日志

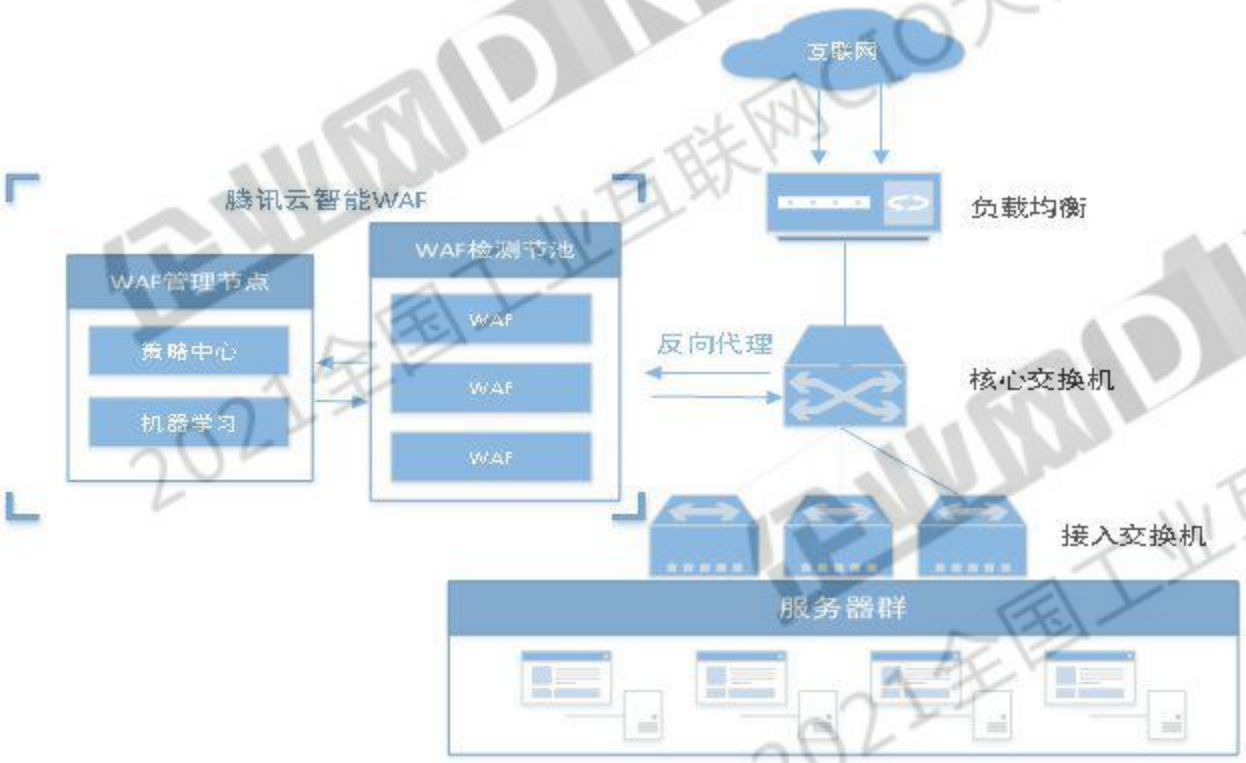
应用安全运营中心
- 用户风险
- 应用风险
- 安全合规
- 应用安全态势

配套能力与服务
- 威胁情报服务
- 专家服务

云计算基础设施：私有云　公有云　混合云　其他部署方式

从外挂“灭火器”到“集成式烟感”

平台和应用安全：web安全



基于AI和规则双引擎，通过分布式弹性架构，结合腾讯威胁情报，解决客户网站入侵， 漏洞利用，挂马，篡改，后门，BOT爬虫，CC攻击、快速扩容等问题。

规则+AI双检测引擎
CC攻击防护
信息泄露控制
BOT行为管理
信息泄露防护

高可用故障迁移

- WAF多节点集群，故障快速迁移及恢复，避免单点故障问题

防护能力弹性伸缩

- 通过增加或减少WAF引擎节点服务器，实现防护能力按需灵活弹性伸缩。

平台和应用安全：主机安全

- 核心资产可量化管理，优化漏洞治理，完善入侵发现机制

主机全生命周期风险管控

解决问题：服务器一旦被黑客入侵，企业面临严峻安全风险

Agent 主机探针 + Engine 安全引擎 + Console 控制中心

40,000+ 高价值漏洞库
30+ 应用弱密码识别
漏洞应急时间 <24h
有效减少90%被攻击面

安全资产清点

安全风险发现

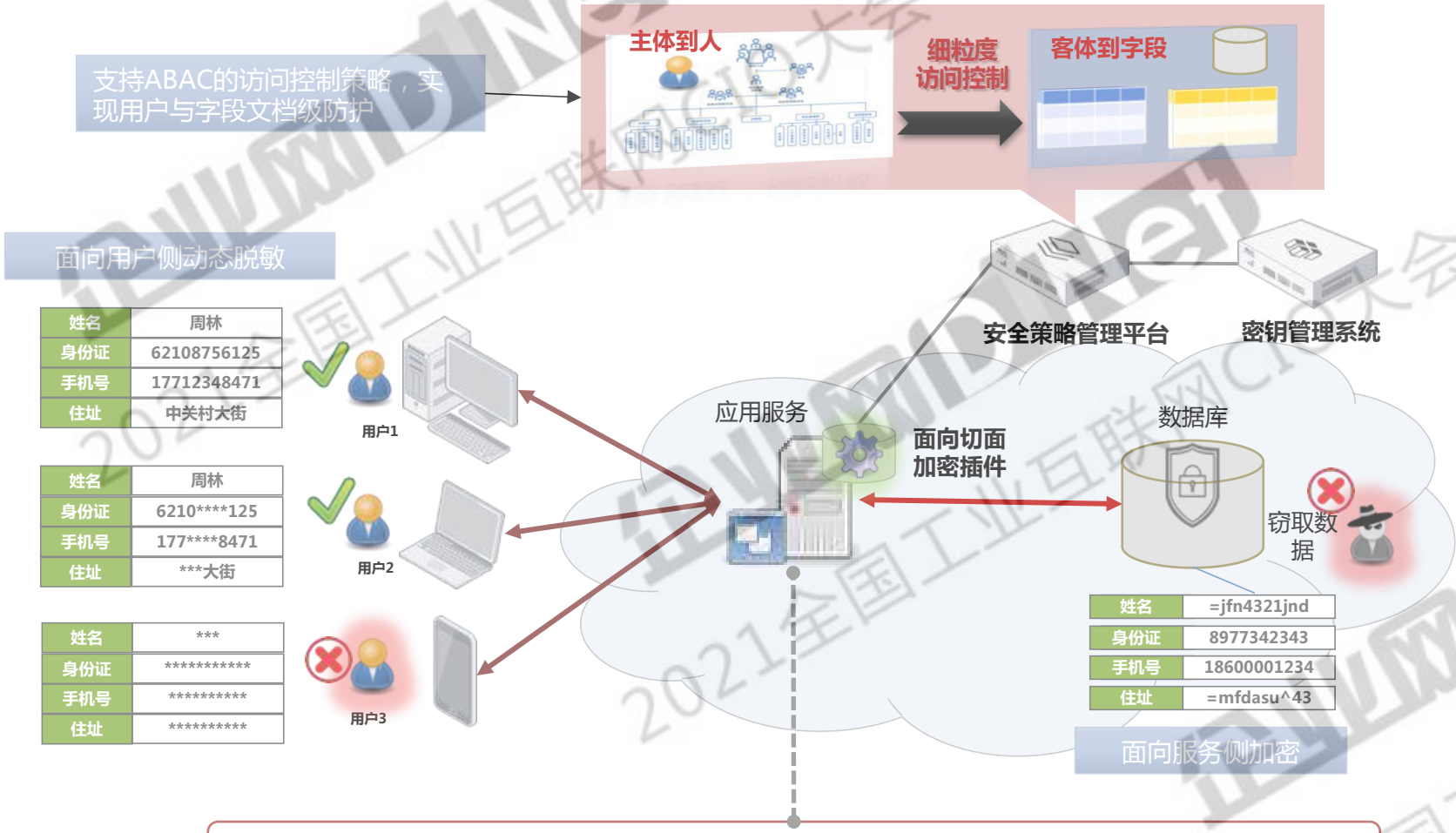
异常登录检测

合规基线核查

构建了由"国内信息安全等级保护"和"CIS"组成的基准要求，涵盖多个版本的主流操作系统、web应用、数据库等

- 新业务系统上线安全检查
- 合规性安全检查
- 日常安全检查

平台和应用安全：数据安全



数据发现：
- 元数据提取、数据扫描
- 特定数据发现（如个人信息）

数据加密：
- 字段或文档级加密
- 锚点解密的防绕过细控与审计

行为审计：
- 可定责的日志防篡改审计
- 数据访问风控

访问控制：
- 基于属性和角色的访问控制
- 丰富的数据脱敏策略

【应对威胁】

1. 服务侧存储加密：防范恶意DBA、外包人员等内部威胁，以及外部黑客
2. 用户侧动态脱敏：防范内部业务人员越权等

【方案优势】

1. **免开发改造应用**，敏捷实施数据加密防护
2. **结合用户身份解密细控，且不改变用户操作习惯**

网络通信安全：接入安全

工业智能网关：采用软硬一体形式，可进行7层内容过滤，支持对工业协议的深度过滤

1 数据采集 | 2 数据传输安全 | 3 网关功能 | 4 边缘计算 | 5 安全运营

支持多种工业设备

PLC
变频器
传感器
RFID
工控机
数控系统
机器人
摄像头

支持多种工业协议

Profibus
Modbus
Ethernet TCP
OPC
……

设备接入身份认证

数据加密传输

入侵检测与防护

支持多种通讯方式

以太网
WIFI
NB-IoT
4G/5G
Zigbee
LORA
……

数据处理

数据本地计算与处理
数据存储
第三方API接口

安全管理

资产识别及可视化
安全监测及预警
安全策略远程部署
安全防护与审计

边缘侧数据采集的安全问题

- 从生产现场到云端的数采安全
- 从生产现场到边缘服务器的数采安全
- 从边缘服务器到云的数采安全

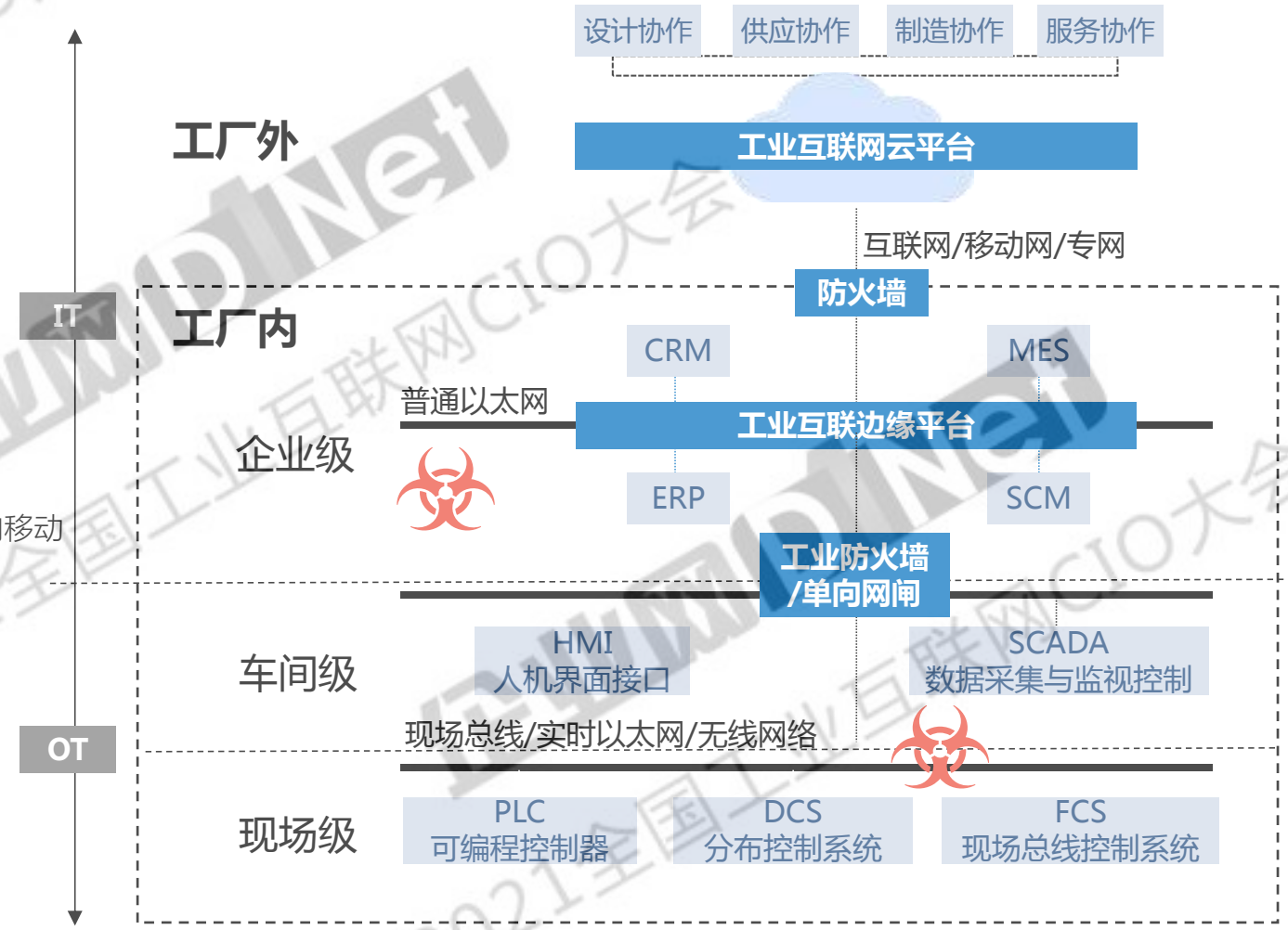
网络通信安全：分区分域，纵深防护

网络层面的威胁分析：

- 通过网络扫描或局域网扫描来发现主机
- 通过暴力破解尝试进入其他主机
- 结合漏洞利用横向移动来感染其他主机
- 通过内部服务器、主机的边界连接来进入内网
- 利用DNS进行C&C通信

安全建设思路：

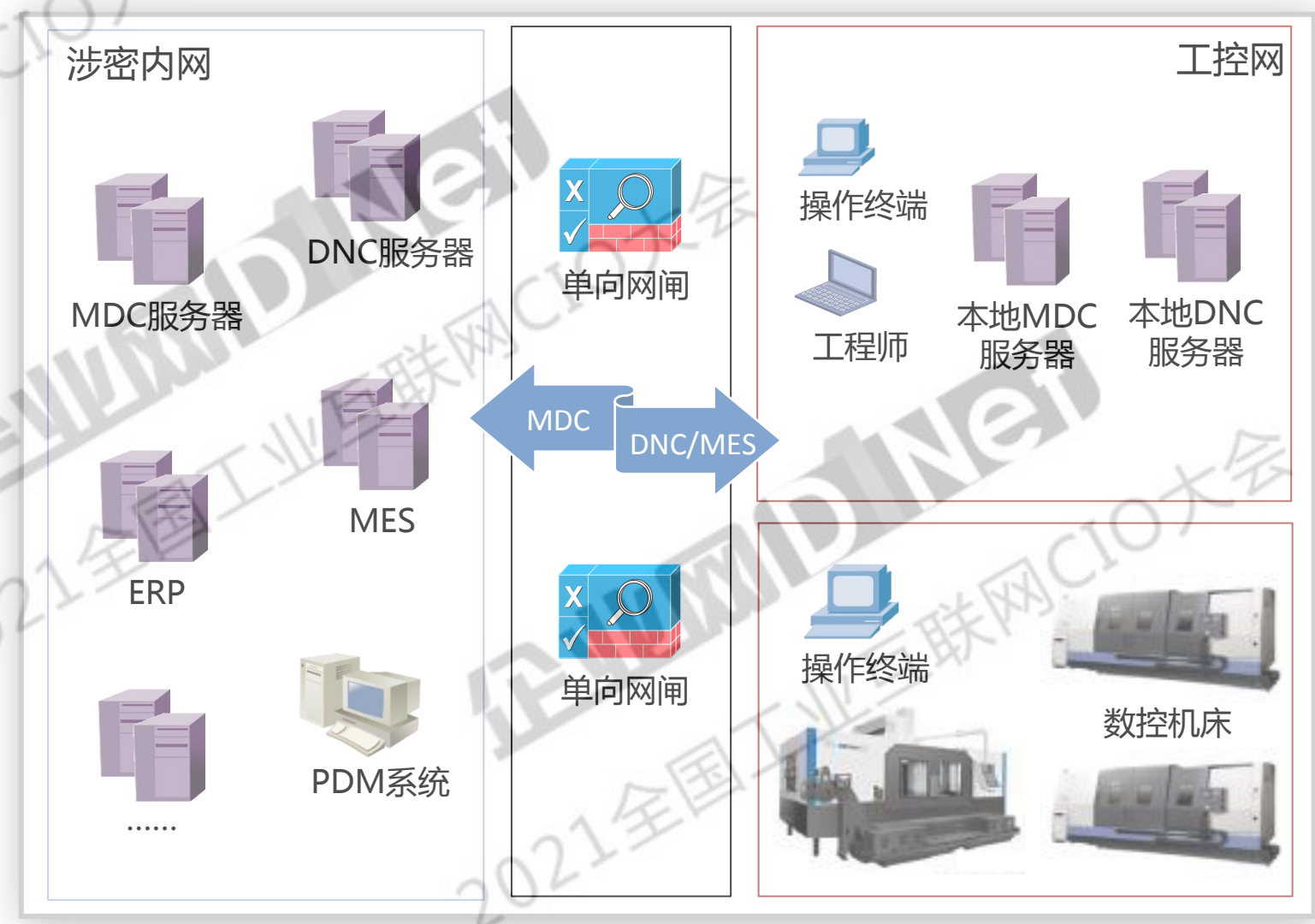
- **划分安全域**，做好访问控制，阻止攻击流量、病毒木马横向移动
- 阻断恶意流量和通道
- 让合法的应用以**加密**的通道进行通信
- 监控、审计和检测网络流量，用于病毒木马事件分析
- 深度包检测



网络通信安全：办公网与生产网隔离与防护控制

在工控网和办公网之间部署单向网闸和防火墙系统，对网络之间的数据访问进行访问控制。

- 办公网DNC服务器程序代码下发至工控网络须通过单向网闸进行控制；
- 工控网络MDC服务器采集数据上传至办公网（涉密内网）也须通过单向网闸进行控制；
- 办公网（涉密内网）与工控网络之间MES生产管理数据通信须通过单向网闸进行控制。

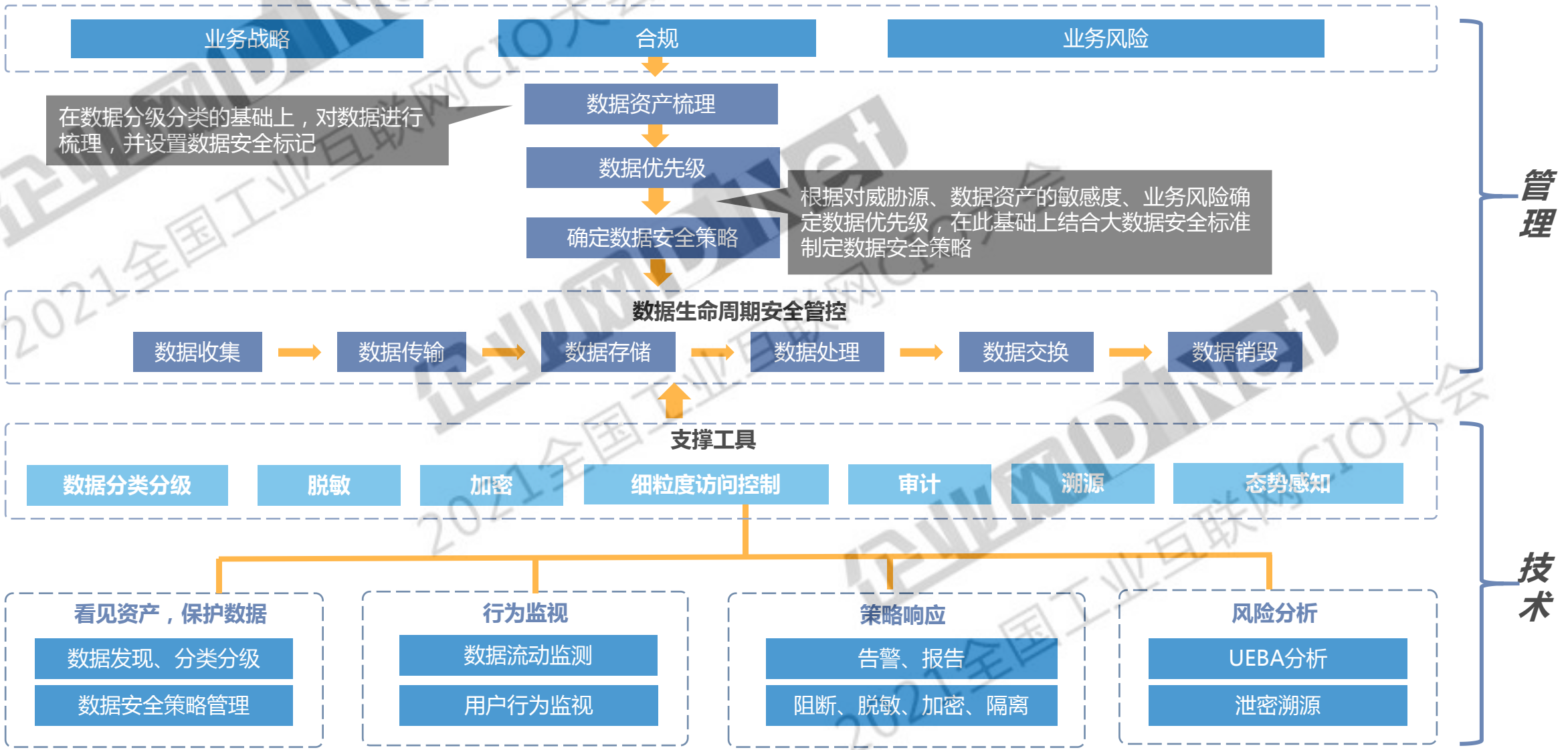


网络通信安全：生产网内部隔离

工控网络生产控制层（DNC/MDC/上位机）与现场设备层（机床CNC/PLC）之间通信须通过工控防火墙进行控制。

- 实现协议指令级控制，实时阻断非法工控协议指令；
- 确保NC文件/G/M代码指令文件传输安全；
- 基于黑白名单防御策略，实时阻断异常行为和非法数据，切断针对CNC/PLC等现场设备的漏洞利用攻击。

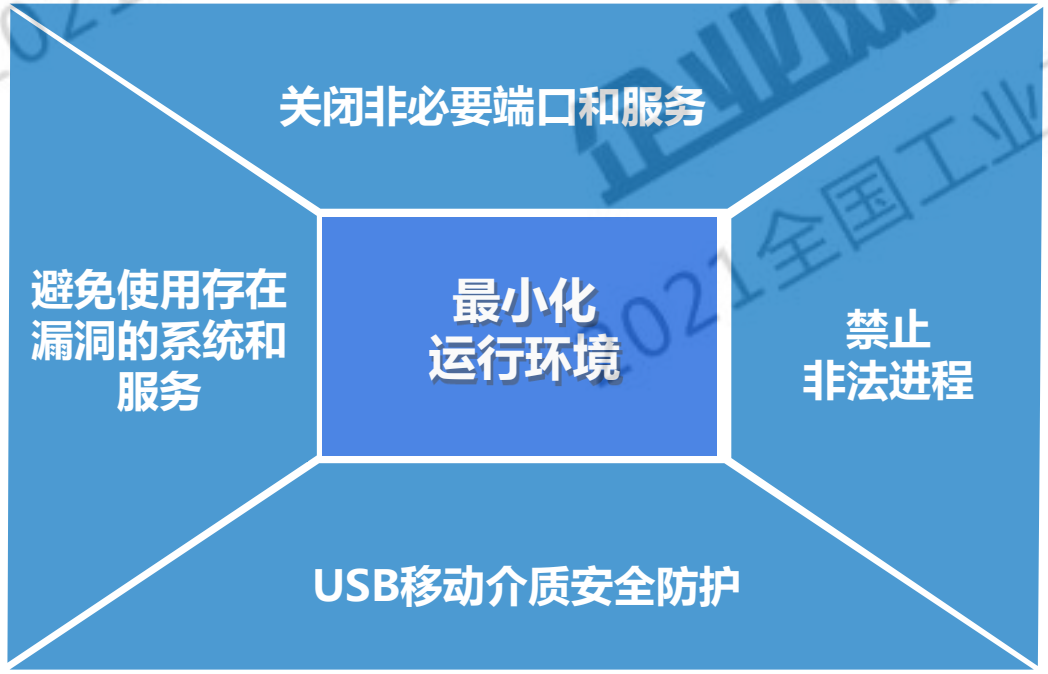
工业数据安全：数据安全治理整体架构



设备与控制安全：工控主机安全设计

确保工控网络内部最小化运行环境，在工控主机上安装主机安全防护软件

- 关闭非必要的端口和服务，避免使用存在漏洞的服务；
- 上位机、运维主机应用程序白名单，通过白名单管理，禁止非法进程运行；
- 上位机、运维主机应用USB移动介质白名单与权限管理，管理移动介质权限，阻止外部攻击者入侵和内部违规访问行为。



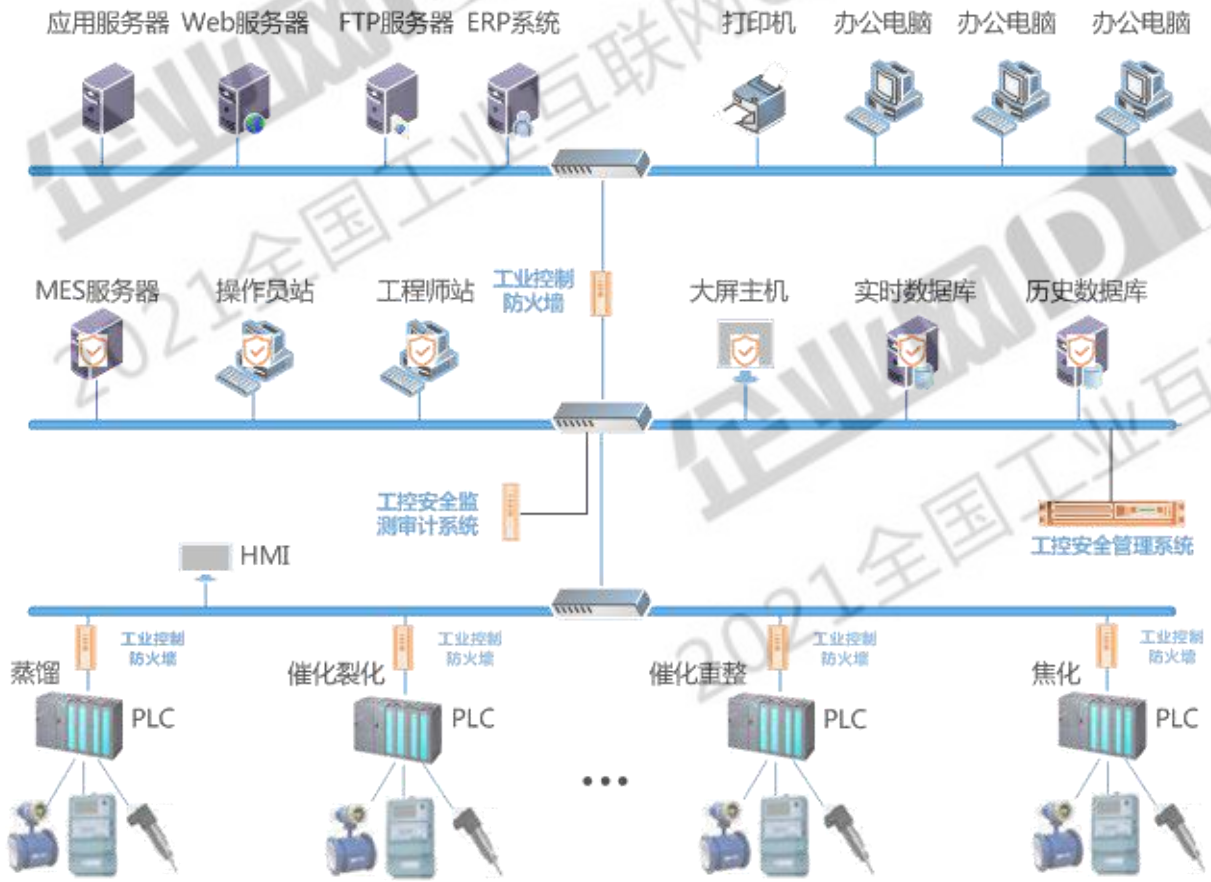
设备与控制安全：漏洞扫描与配置核查

- 上位机、DNC/MDC服务器系统漏洞扫描与补丁管理；
- CNC/PLC等工控设备漏洞扫描；
- 上位机、运维主机、DNC/MDC服务器安全配置核查。

Honeywell XL Web II Controller...	高
HollySys软件HT8000工程文件存在...	中
Advantech WebAccess安全绕过漏洞...	中
Advantech WebAccess 'updateTem...	高
GE组态软件iFIX V5.8存在远程拒绝...	中
Rockwell Automation Logix5000 ...	高
Rockwell Automation MicroLogix...	中
Rockwell Automation MicroLogix...	中
Scada-os组态软件工程文件存在缓...	中
施耐德140NOE77101以太网模块存在...	中
PLC WinProladder栈缓冲区溢出漏...	中
siemens 840D存在远程溢出漏洞	高
SIMATIC S7-300和S7-400 CPU拒绝...	中

系统服务	检查WINDOWS主机是否开启了不必要的	对系统运行的服务应该进行严格控制，一些不应该开启的服务或是会带来
安全配置	检查屏幕保护程序安全配置	启用屏幕保护程序，防止管理员忘记锁定机器被非法攻击；设置带密码的
	检查是否安装防病毒软件	检查windows设备是否安装了统一部署的防病毒软件
	RDP协议	1.RDP访问协议加密
	远程注册表	禁用可远程访问的注册表路径和子路径
	FTP安全	1、控制FTP进程缺省访问权限，当通过FTP服务创建新文件或目录时应将
	信息泄露	禁对rpc、DCE/RPC服务枚举调查
	检查是否开启防火墙	启用自带防火墙或安装第三方威胁防护软件，根据业务需要限定允许访问
	NTFS格式	检查磁盘分区格式是否为NTFS格式
访问控制	检查Windows系统的共享是否禁用；	检查有无自建的共享目录。
	检查远程连接工具配置安全	检查WINDOWS系统的远程桌面是否开启，如果开启，检查是否MS12-
	检查远程关机配置安全	在本地安全设置中从远端系统强制关机只指派给Administrators组。
	检查本地关机配置安全	在本地安全设置中关闭系统仅指派给Administrators组。
	检查用户权利指派配置安全	在本地安全设置中取得文件或其它对象的所有权仅指派给Administrators
	远程管理地址安全要求	对于通过IP协议进行远程维护的设备，设备应支持对允许登陆到该设备的
	禁止不安全的管理方式	禁止使用telnet远程管理；

设备与控制安全：工控系统安全监测审计



- 支持多种**工控协议**的深度解析、访问控制、过滤、审计和检测

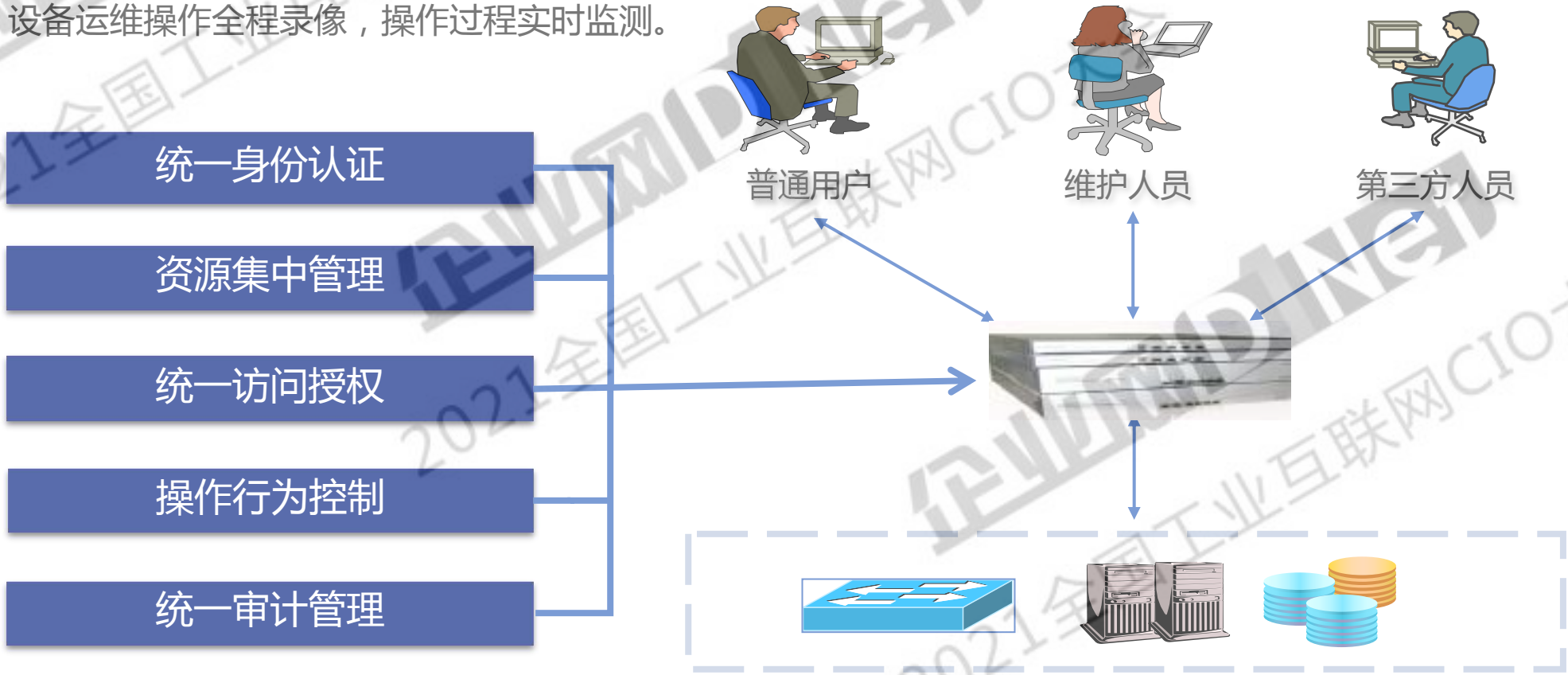
（IEC60870-5-101/104、Modbus TCP、Profinet、Siemens S7、DNP3、Ethernet/IP、OPC、MMS、MBTP、EIP、OPC、DNP3.0、IEC104、IEC61850、、BacNet ..... ）

- 基于工控白名的单**指令读写控制**。支持工业协议访问控制，对指令读写进行控制，保护工控设备
- 支持对DDoS攻击、扫描攻击以及漏洞利用攻击进行防护，支持对**工控网络和应用入侵防护**
- **异常检测**。可记录发送到/来源于现场设备的所有的指令和指令执行结果，进行全面的深度分析和异常行为检测，提供现场设备故障报警和恶意入侵活动报警
- **可视化**展示：直观展示工控网络拓扑图，提供可视化的异常展示与告警

设备与控制安全：设备操作运维管理

在工控网内部署设备运维堡垒主机，实现操作人员设备运维操作的管理。

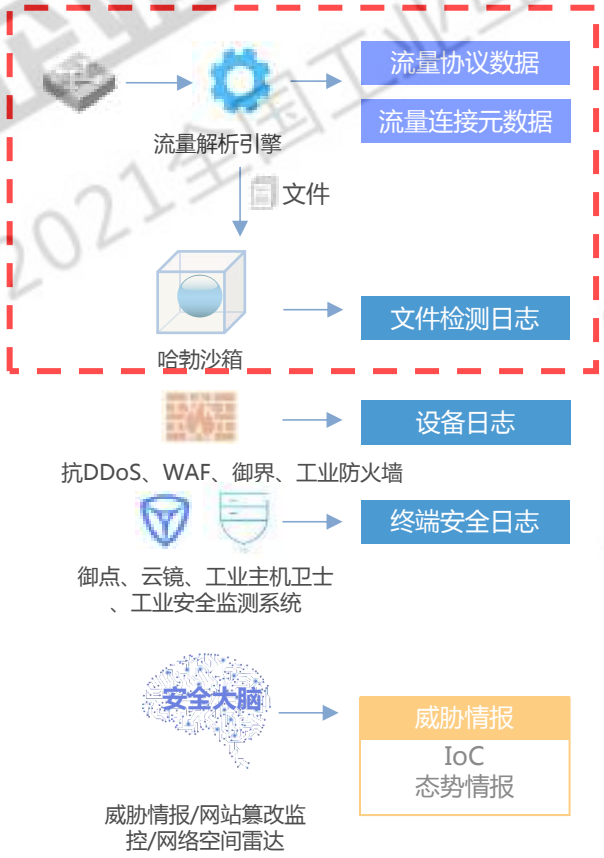
- 操作运维实名制管理；
- 操作运维命名黑白名单管理，实现最小化授权；
- 设备运维操作全程录像，操作过程实时监测。



IOT安全运营中心：整体架构

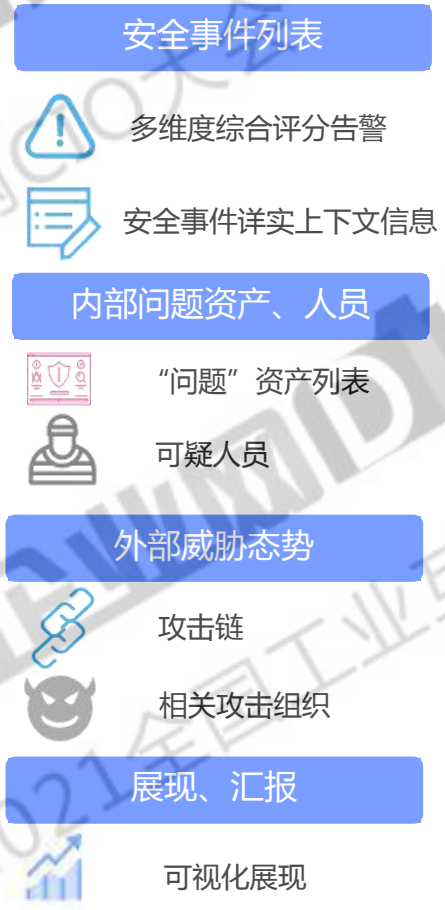
IOT安全运营中心基于大数据技术的监控预警平台，在IOT资产统一管理基础上，对工业企业面临的外部攻击威胁和内部脆弱性风险进行深度检测，提供威胁检测、分析、预警、处置的能力，实现企业全网安全态势可知、可见、可控的闭环。

IOT安全数据采集



智能大数据平台

输出



解决问题

威胁能感知

家底什么样：哪些IOT资产最危险，影响哪些业务

谁在攻击我：威胁情报、统计分析了解攻击者信息

怎么攻击我：已知威胁、未知威胁、安全事件及上下文信息

事件处理快

太多安全事件，先处理哪个

事件之间有什么关系

绩效看得到

企业面临的威胁态势，做了哪些工作一目了然

IOT安全运营中心：整体安全态势感知

- **工业风险态势**

对全网资产面临的脆弱性、攻击事件、通报处置情况进行多维度分析综合展示

- **工业威胁态势**

对攻击威胁源头进行多维度分析综合展示

- **工业资产地图**

—对要保护的资产、保护设备、保护人力进行多维度分析综合展示

- **工业通报态势**

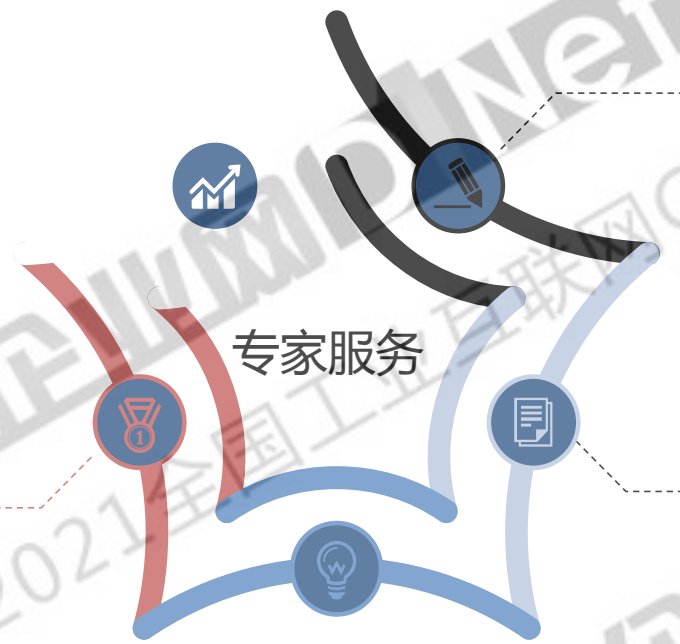
对告警处置情况进行多维度分析综合展示

安全服务：安全服务市场

由专业的安全专家团队提供安全咨询、渗透测试服务、应急响应、安全托管等服务，帮助工业企业获得合适的安全解决方案、发现潜在安全威胁和提升用户的安全防护能力、帮助用户恢复业务，定位黑客身份。

工业互联网安全咨询

依据国家政策和国家信息安全标准，基于客户信息安全需求，提供企业信息安全规划与管理方面的安全咨询。协助企业识别信息资产及业务流程的信息安全弱点，并针对信息安全威胁提供信息安全风险处理规划建议。



工业互联网风险评估/攻防演练

提供工业漏洞扫描、渗透测试等安全风险评估服务。提供模拟真实环境的红蓝对抗应演练服务，急时发现问题。

应急响应

一旦发生安全事件及时预警并提供安全应急方案和技术支持，协助用户应对突发安全事件，更为用户提供突发安全事件分析报告和安全状况分析报告，协助用户应对突发安全事件，降低损失,消除用户的后顾之忧。

安全托管服务

提供的安全运营服务，使用三阶共享专家模式，提供7X24小时持续服务，持续帮助用户单位持续监测安全状态；并在安全事件发生前、发生时、发生后动态调整安全策略，使被保单位的安全防护能力逐步提升，持续优化运营机制，由被动运维逐步转向主动运营。

4 腾讯安全能力简介

- **腾讯安全能力介绍：**涉及到腾讯安全能力简介，包括人员、技术、产品等维度
- **相关案例说明：**部分工业互联网安全案例说明

腾讯安全业务矩阵

四大业务矩阵

01 互联网安全大数据矩阵

- 腾讯安全云库
- 互联网+警务LBS大数据
- 腾讯麒麟伪基站实时检测系统
- 腾讯鹰眼智能反电话诈骗系统
- 腾讯神荼反欺诈盒子
- 腾讯神侦资金流查控系统

02 市场领先安全产品矩阵

腾讯2C安全

- 腾讯手机管家
- 腾讯电脑管家
- 腾讯WiFi管家
- 腾讯御安全
- 同步助手
- 相册管家

腾讯产业安全

- 云安全
- 业务安全
- 大数据安全
- 移动安全
- 终端安全
- 物联网安全
- 安全服务

03 腾讯安全实验室矩阵

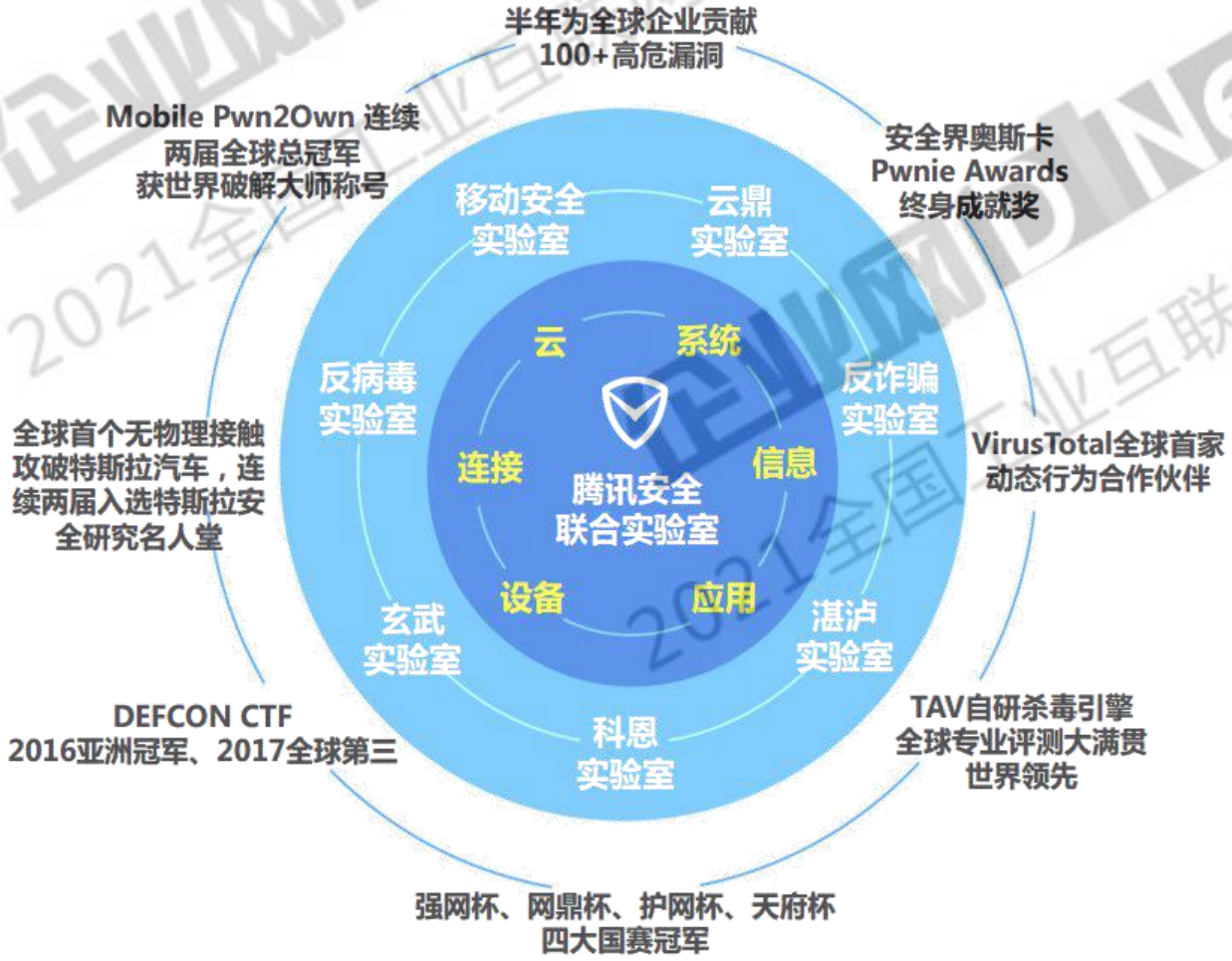
- 腾讯安全科恩实验室
- 腾讯安全玄武实验室
- 腾讯安全湛泸实验室
- 腾讯安全云鼎实验室
- 腾讯安全反诈骗实验室
- 腾讯安全反病毒实验室
- 腾讯安全移动安全实验室

04 安全行业联盟矩阵

- 腾讯守护者计划
- CSS中国互联网安全领袖峰会
- TCTF腾讯信息安全争霸赛
- GeekPwn极客大赛
- 腾讯领御守护计划
- 上市公司安全联盟

七大安全实验室，TOP级安全对抗及研究能力

七大实验室 斩获国际荣誉



实践应用成果

- 腾讯安全联合实验室承担“国家重点研发计划” 两大课题
- 公安部授予“公安部打击治理电信网络新型违法犯罪防控中心”
- 与国家工商总局共同成立“网络传销深圳监测中心”
- 与浙江省公安厅共建安全联合实验室
- 携手上海市成立“腾讯上海反电信网络诈骗联合实验室”
- 与深圳公安共同建立了国内首个实体“金融安全实验室”
- 与重庆市网信办共同成立“腾讯重庆网络大数据实验室”
- 与广州、西安、武汉、北京、上海、山东等地开展校企联合培养网安人才
- 2015年开始，每年持续为春节微信红包活动提供安全保障能力
- 国家信息安全漏洞共享平台授予“原创漏洞报送突出贡献单位”奖
- 腾讯安全玄武实验室“阿图因”系统入选世界互联网大会领先科技成果
- 发掘微软、谷歌、Adobe、苹果、宝马、特斯拉等国际厂商的安全漏洞，并提供了修复建议，获数百次公开致谢，位居国内首位
- 发掘华为手机和路由器、支付宝APP、360手机浏览器等国内知名厂商的重大漏洞，并提供修复建议
- 5秒攻破苹果Safari浏览器，并获Root权限； 4次秒破微软Edge浏览器；8秒攻破苹果iOS10.1，iphone X iOS 11.1.1系统正式发布不到10小时，在全球范围内首次被成功越狱； 10秒攻破谷歌Nexus 6P手机

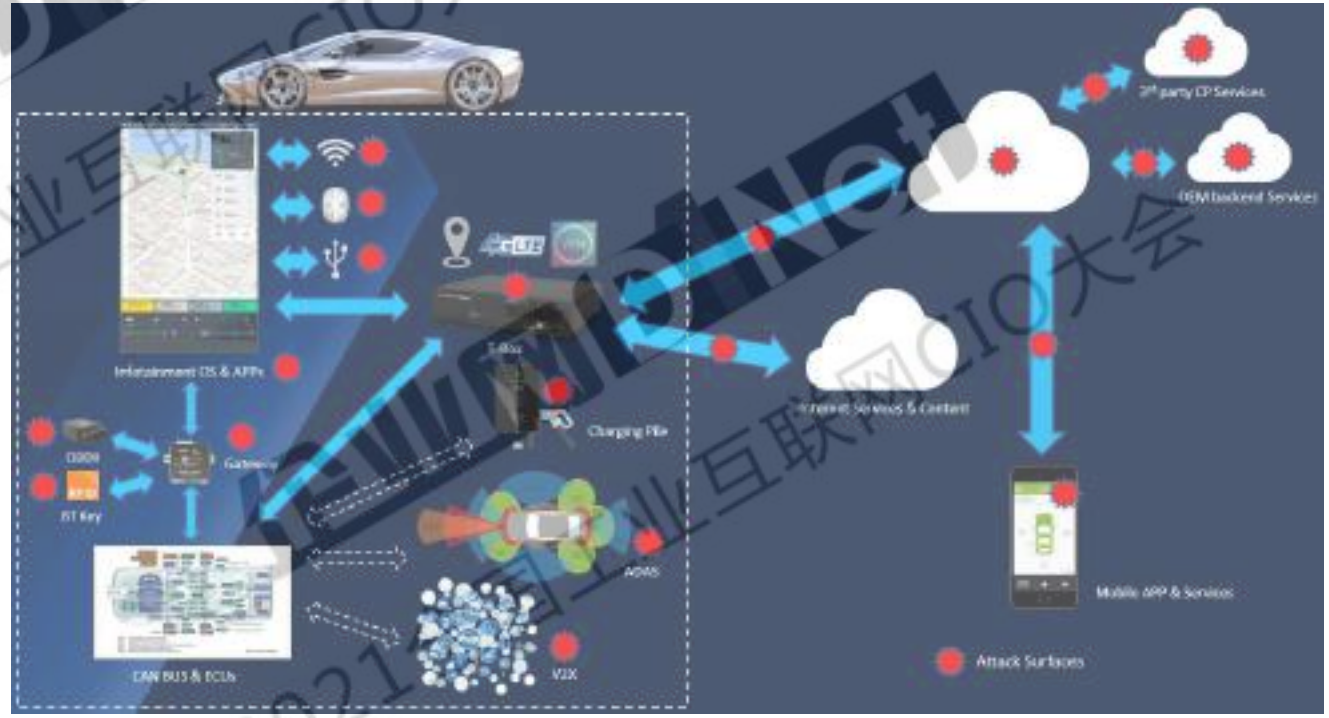
IOT安全能力获得特斯拉认可

特斯拉有史以来最高安全研究奖励

Tesla Security Researcher Hall of Fame

Tesla appreciates and wants to recognize the contributions of security researchers. If you are the first researcher to report a confirmed vulnerability, we will list your name in our Hall of Fame (unless you would prefer to remain anonymous). You may also be considered for an award if you are the first researcher to report one of the top 3 confirmed vulnerabilities in a calendar quarter. You must comply with our Responsible Disclosure Guidelines (above) to be considered for our Hall of Fame and top 3 awards.

2017	Keen Security Lab	Tencent
2016	Keen Security Lab	Tencent



富士康工业互联网案例：三大连接深度融合

腾讯云 | 工业互联网安全

技术连接：运营技术（OT）+ 信息技术（IT）

双方联合研发和构建面向工业互联网的基础设施平台，多地多中心部署保障跨地域业务无缝接入，并针对工业互联网多租户、多场景、按次计费等需求，与富士康联合进行创新工业PaaS平台创新，形成灵活扩展，开发运营一体化的先进工业互联网平台，加速富士康工业科技能力输出

安全连接：厂端安全+云端安全

面对工业互联网安全新挑战，结合富士康厂端安全架构和腾讯云端全链路安全能力，打造高度安全的纵深防护体系，为用户数据和平台运行提供全方位的安全保障

生态连接：富士康产业生态+腾讯互联网生态

将腾讯亿级用户，企业微信，合作伙伴及开发者生态进行共享，为富士康量身定做工业互联网开发者中心，进行生态导入和宣传，形成集约化的产业势能传递生态链条，快速扩大影响力

工业安全

- 业务安全
- 应用安全
- 数据安全
- 主机安全
- 网络安全
- 云安全
- 物理安全

工业SaaS

设计应用 | 生产应用 | 供应链应用 | 智能运维 | 企业微信 | 商业分析 | 数据可视化 | 智能缺陷检测 | 智能营销

工业PaaS

- 工业微服务组件库：工业知识组件、算法组件、设备模型
- 工业数据建模：数据分析、机理模型
- 运维运营平台：计费管理、运维管理、运营管理、多租户服务
- 应用开发框架：微服务框架、开发工具、消息队列
- 工业大数据平台：大数据处理套件、机器学习平台

IaaS平台

公有云/TCE专有云/混合云/多云管理 | 大数据传输和存储

物联网平台

设备接入 | 认证鉴权 | 设备管理 | 规则引擎 | 边缘网关/边缘计算

机器人 | 离散制造 | 数控机床 | 汽车 | 钢铁 | 电力能源 | 高端装备 | 石油化工 | 流程制造

谢谢聆听！

Tencent 腾讯 | 腾讯云